ars TECHNICA

Cyrus Farivar <cyrus.farivar@arstechnica.com>

JUSTICE DEPARTMENT ANNOUNCES COURT-AUTHORIZED EFFORTS TO MAP AND DISRUPT BOTNET USED BY NORTH KOREAN HACKERS

1 message

USDOJ-Office of Public Affairs <USDOJ-OfficeofPublicAffairs@public.govdelivery.com> Wed, Jan 30, 2019 at 10:48 AM
Reply-To: USDOJ-OfficeofPublicAffairs@public.govdelivery.com
To: cyrus.farivar@arstechnica.com

FOR IMMEDIATE RELEASE
WEDNESDAY, JANUARY 30, 2019

Note: A copy of the warrant and order can be found here. A copy of the application can be found here.

JUSTICE DEPARTMENT ANNOUNCES COURT-AUTHORIZED EFFORTS TO MAP AND DISRUPT BOTNET USED BY NORTH KOREAN HACKERS

WASHINGTON – The Justice Department today announced an extensive effort to map and further disrupt, through victim notifications, the Joanap botnet – a global network of numerous infected computers under the control of North Korean hackers that was used to facilitate other malicious cyber activities. This effort targeting the Joanap botnet follows charges unsealed last year in which the United States charged a North Korean citizen, Park Jin Hyok, a member of a conspiracy backed by the North Korean government that carried out numerous computer intrusions. Those charges alleged that the conspiracy utilized a strain of malware, "Brambul," which was also used to propagate the Joanap botnet.

Assistant Attorney General for National Security John Demers, United States Attorney Nicola T. Hanna, Assistant Director in Charge (ADIC) Paul Delacourt of the FBI's Los Angeles Field Office and the U.S. Air Force Office of Special Investigations made the announcement.

"Computers around the world remain infected by a botnet associated with the North Korean Regime," said Assistant Attorney General Demers. "Through this operation, we are working to eradicate the threat that North Korea state hackers pose to the confidentiality, integrity, and availability of data. This operation is another example of the Justice Department's efforts to use every tool at our disposal to disrupt national security threat actors, including, but by no means limited to, prosecution."

"Our efforts have disrupted state-sponsored cybercriminals who used malware to establish a computer network that gave them the ability to hack into other computer systems," said U.S. Attorney Hanna. "While the Joanap botnet was identified years ago and can be defeated with antivirus software, we identified numerous unprotected computers that hosted the malware underlying the botnet. The search warrants and court orders announced today as part of our efforts

to eradicate this botnet are just one of the many tools we will use to prevent cybercriminals from using botnets to stage damaging computer intrusions."

"Through technical means and legal process, the FBI continually seeks to disrupt the malicious cyber activities of North Korean cybercriminals, as in this case, and all cyber actors who pose a threat to the United States and our international partners," said ADIC Delacourt. "We urge computer users to take precautions, such as updating their software and utilizing antivirus, in order to avoid being victimized by this type of malware."

Joanap malware targeted computers running the Microsoft Windows operating system and is used to gain access to and maintain infrastructure from which the hackers can carry out other malicious cyber activities. Joanap is a "second stage" malware, one that is often "dropped" by the automated Brambul "worm" that crawls from computer to computer, probing whether it can gain access using certain vulnerabilities. Once installed on an infected computer, Joanap would allow the North Korean hackers to remotely access infected computers, gain root level (or near-total) access to infected computers, and load additional malware onto infected computers.

Computers infected with Joanap — known as "peers" or "bots" — became part of a network of compromised computers known as a botnet. Like other botnets, Joanap was designed to operate automatically and undetected on victims' computers. Joanap uses a decentralized peer-to-peer communication system, rather than a centralized mechanism to communicate with and control the peers, such as a command-and-control domain.

In order to address that distinct feature, a court order and search warrant was obtained pursuant to recent amendments to Rule 41 of the Federal Rules of Criminal Procedure. The search warrant allowed the FBI and AFOSI to operate servers that mimicked peers in the botnet. By pretending to be infected peers, the computers operated by the FBI and AFOSI under the authority of the search warrant and order collected limited identifying and technical information about other peers infected with Joanap (*i.e.*, IP addresses, port numbers, and connection timestamps). This allowed the FBI and AFOSI to build a map of the current Joanap botnet of infected computers. Copies of the search warrants and orders and applications are available below.

Using the information obtained from the warrant, the government is notifying victims in the United States of the presence of Joanap on an infected computer. The FBI is both notifying victims through their Internet Service Providers and providing personal notification to victims whose computers are not behind a router or a firewall. The U.S. government will coordinate the notification of foreign victims by contacting the host country's government, including by utilizing the FBI's Legal Attachés.

The second-stage Joanap botnet and the first-stage Brambul worm have endured since 2009, even though they have been identified in the past and a number of antivirus products defend against them. Many private cyber security research companies have also published analytical reports about Brambul and Joanap. The FBI and the Department of Homeland Security have published reports analyzing Joanap and Brambul as well, including as recently as May 31, 2018. (https://www.us-cert.gov/ncas/alerts/TA18-149A.) Moreover, a complaint was filed on June 8, 2018, charging Park Jin Hyok with a conspiracy to carry out numerous computer intrusions backed by the North Korean government. That complaint alleged how co-conspirators used Brambul to gain unauthorized access to computers, and then used those computers to carry out the charged malicious cyber activities. The Brambul worm itself was recovered from the computer networks of some victims of the conspiracy.

Joanap targets Microsoft Windows operating systems, but running Windows Defender Antivirus and using Windows Update will remediate and prevent infections by Joanap. A number of free and paid antivirus programs are also already capable of detecting and removing Joanap and Brambul, including the Microsoft Safety Scanner, a free product.

This effort to map and disrupt the botnet was led by Assistant United States Attorneys Anthony J. Lewis and Anil J. Antony of the United States Attorney's Office for the Central District of California, and DOJ Trial Attorneys David Aaron and Scott Claffee of the National Security Division's

Counterintelligence and Export Control Section. The Criminal Division's Computer Crime and Intellectual Property Section provided valuable assistance.

The details contained in the application for the search warrant and order and related pleadings are not charges and are merely accusations.

# # #

NSD

19-24

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.